WHAT IS CLAIMED IS

1. A method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a mobile network security system including a serving interface operatively connected to the serving node, a gateway interface operatively connected to the gateway node, a processor and a memory,

wherein the data packets and the signal packets pass through said serving interface and said gateway interface, wherein said mobile network security system monitors the creation, updating and destruction of the tunnel by monitoring the signal packets;

(b) reading by said processor the reference to the protocol context of at least one of said data packets; and

(c) applying a policy based on a tunnel profile, thereby performing at least one action to said at least one of the data packets, wherein said at least one action is based on the payload, wherein said tunnel profile is selected based on at least one of the identifiers carried in the protocol context.

2. The method, according to claim 1, further comprising the step of, prior to said applying:

(d) storing in said memory a tunnel context based on the protocol context, wherein said tunnel context includes said at least one of the identifiers.

3. The method, according to claim 1, further comprising the steps of, prior to said applying:

(d) storing said tunnel profile in said memory.

4. The method, according to claim 1, wherein said at least one of the identifiers is selected from the group consisting of an access point name, a user name and a telephone number for each of the mobile stations.

5. The method, according to claim 2, further comprising the steps of:

(e) updating said tunnel context based on at least one change of the protocol context, and storing a modified tunnel context; and

(f) updating said tunnel profile based on said modified tunnel context.

6. The method, according to claim 1, wherein said tunnel profile is further based on information from an external data base.

7. The method, according to claim 6, wherein said external data base is included in an external system selected from the group consisting of fraud management systems, charge and billing systems, account management and authentication servers.

8. The method, according to claim 1, wherein said applying a policy provides a service selected from the group consisting of security checking, bandwidth management, quality of service, virtual private network, extended security checking, intrusion detection and prevention, and voice over Internet protocol, wherein said service is selected based on said tunnel profile.

9. The method, according to claim 8, wherein said service is differentiated respectively to each of the mobile stations based on said tunnel profile.

10. A method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data

communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a mobile network security system including an interface to the mobile data network, a processor and a memory,

wherein said mobile network security system monitors the creation, updating and destruction of the tunnel by monitoring the signal packets,

(b) reading by said processor the reference to the protocol context; and

(c) querying by a management system for information stored in the protocol context.

11. A method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a mobile network security system including an interface to the mobile data network, a processor and a memory,

wherein said mobile network security system monitors the creation, updating and destruction of the tunnel by monitoring the signal packets,

(b) reading by said processor the reference to the protocol context; and

(c) sending commands to destroy the data packets of the tunnel wherein the tunnel is in use by an unauthorized mobile station, whereby the data packets are identified based on said protocol context.

12. A system which provides security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein the protocol context of the tunnel is communicated by at least one of the signaling packets, the system comprising:

(a) a serving interface operatively connected to the serving node;

(b) a gateway interface operatively connected to the gateway node;

wherein the data packets and signaling packets pass through said serving interface and said gateway interface;

(c) a processor which reads the reference to the protocol context of at least one of said data packets; and

(d) a memory mechanism;

wherein said processor selects a policy based on a tunnel profile previously stored with said memory mechanism, said processor thereby performs at least one action to said at least one of the data packets, wherein said at least one action is based on the payload, wherein said tunnel profile is selected based on at least one of the identifiers carried in the protocol context.

13. The system, according to claim 12, wherein said memory mechanism further stores a tunnel context based on the protocol context, wherein said tunnel context includes said at least one of the identifiers.

14. The system, according to claim 12, further comprising:

(e) a management interface, operatively connected to a management system for querying information stored in the tunnel context.

15. The system, according to claim 12, wherein said at least one of the identifiers is selected from the group consisting of an access point name, a user name and a telephone number of said mobile station.

16. The system, according to claim 13, wherein said processor updates said tunnel context based on at least one change of the protocol context, and thereby stores with said memory mechanism a modified tunnel context, and said processor updates said tunnel profile based on said modified tunnel context.

17. The system, according to claim 13, wherein said processor updates said tunnel context based on the mobile station roaming to a second serving node.

18. The system, according to claim 13, wherein said processor destroys a tunnel context by commanding at least one node selected from the group consisting of serving nodes and gateway nodes to destroy the tunnel.

19. The system , according to claim 12, further comprising:

(e) an external database, wherein said tunnel profile is further based on information from said external data base.

20. The system, according to claim 19, wherein said external data base is included in an external system selected from the group consisting of fraud management systems, charge and billing systems, account management systems and authentication servers.

21. The system, according to claim 12, wherein said policy provides a service selected from the group consisting of security checking bandwidth management, quality of service, virtual private network, extended security checking, intrusion detection and prevention and voice over Internet protocol; wherein said

service is selected based on said tunnel profile; wherein said service is differentiated respectively to each of the mobile stations based on said tunnel profiles.

22. A method for providing security during roaming and handoff from a first mobile data network to a second mobile data network, each network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a first mobile network security system to the first mobile data network and further providing a second mobile network security system to the second mobile data network, each security system including a serving interface operatively connected to the serving node, a gateway interface operatively connected to the gateway node, a processor and a memory,

wherein the data packets and the signal packets pass through said serving interface and said gateway interface, wherein said first and second mobile network security system monitor the creation, updating and destruction of the tunnel by monitoring the signal packets,

(b) reading the reference to the protocol context of at least one of said data packets by said processor of the first mobile security system; and

(c) storing a tunnel context based on the protocol context in said memory of the first mobile security system, wherein said tunnel context includes said at least one of the identifiers; and

(d) transferring said tunnel context to the second mobile network security system thereby protecting the second mobile data network wherein the

mobile station associated with said tunnel context roams to the second mobile data network.

23. The method, according to claim 22, wherein said transferring said tunnel context occurs prior to the hand-off from the first mobile data network to the second mobile data network.

24. A method for providing security in a mobile data network including a serving node, serving a plurality of mobile stations and undergoing data communications with a gateway node, the data communications transferring data contained in a plurality of data packets encapsulated in a tunnel by the serving node and the gateway node, each data packet including a payload and a reference to a protocol context, the protocol context including a plurality of identifiers for each of the mobile stations using the tunnel, wherein the serving node and gateway node further communicate with each other using a plurality of signaling packets for the creation, updating and destruction of the tunnel, wherein at least a portion of the protocol context of the tunnel is communicated by at least one of the signaling packets, the method comprising the steps of:

(a) providing a mobile network security system including an interface to the mobile data network, a processor and a memory,

wherein said mobile network security system monitors the creation, updating and destruction of the tunnel by monitoring the signal packets,

(b) reading by said processor the reference to the protocol context and at least a portion of the payload of at least one of said data packets; and

(c) applying a policy, thereby performing at least one action to said at least one of the data packets, wherein said at least one action is based on the payload, wherein said at least one action is selected based on at least one of the identifiers carried in the protocol context.

25. A program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 1.

26. A program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 10.

27. A program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 11.

28. A program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 22.

29. A program storage device readable by a machine tangibly embodying a program of instructions executable by the machine for implementing the method of claim 24.